UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,981	08/29/2001	R. Christian Call	29250-002172/US	7532

30594 7590 10/21/2005

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/941,981	CALL ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 26 July 2005 have been fully considered but they are not persuasive.

2. Referring to the rejection of claim 1, the Applicant argues and contends that the prior art Lewis et al. does not teach nor suggest selecting and deleting classified session cache entries. The Examiner respectfully disagrees and asserts that Lewis et al. discloses a method and apparatus for predicting and preventing network attacks, in which data is collected from network devices during an attack. This process allows the administrator of security management to identify the usage levels of different classes of traffic. The collected data selected for cache entries are targeted for pruning (deleting) because the information represents sessions created by an attacker. The pruning mechanism (deleting) is used for cache entries which have exceeded the memory threshold. (See page 12, Section 0120 and page 13, Sections 0130 and 0136). Lewis et al. also discloses by pruning traffic, cache entries for sessions will be part of an attack. (See page 2, Sections 0018-0021)

3. Therefore, the rejection of claims 1-30 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jungck et al. (US Pub No. 2002/0065938) in view of Lewis et al. (US Pub No. 2003/0110396).

Referring the rejection of claims 1,12, and 25, Jungck et al. discloses a method for use with a stateful packet processing device of a computer network for mitigating effects of a network overload against said device, said method operable to free memory used to store information about communications sessions managed by said device, said method comprising the steps of:

classifying session cache entries made in memory into different cache classes, according to one or more characteristics of those entries (See page 10, Section 0080, page 12, Sections 0087-0090)

determining when said device is under network overload (See page 7, Section 0065, page 14, Section 0105) and

determining when sufficient memory has been freed, such that said cache entries are no longer deleted (See page 24, Section 0171)

However, Jungck et al. fail to disclose selecting session cache entries for deletion and deleting (pruning component) them thereby freeing associated memory when said device is under network overload. Lewis et al. discloses the pruning feature for selecting sessions of the packet processing device in accordance with the communication traffic classification and memory threshold. (See page 12, Section 0120,

page 13, Sections 0130 and 0136). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Jungck et al's processing packets system by combining Lewis et al.'s predicting and preventing network attacks method to prevent attacks on network communication devices. One of ordinary skill in the art would have been motivated to do this in order to prevent hackers from overwhelming communication devices with large volumes of data, such as in a Distributed Denial of Service (DDOS). (See Lewis et al. page 2, Section 0021)

Referring to rejection of claims 2 and 14, Jungck et al. as modified discloses wherein said characteristics for said step of classifying are selected from the group consisting of: whether the session is dropped by the device, whether the session is audited by the device, IP protocol of the session, ICMP type and code used in the session, TCP ports used in the session, UDP ports used in the session, and whether the session is a half-open TCP session. (See Lewis et al. page 6, Sections 0068-0069)

Referring to the rejection of claims 3 and 15, Jungck et al. as modified discloses wherein certain of said characteristics of the session may be identified as "any" wherein any session matches a particular criterion for classification. (See Jungck et al. page 11, Section 0084)

Referring to the rejection of claims 4 and 16, Jungck et al. as modified discloses wherein predefined cache classes are selected from the group consisting of:

dropped and unaudited sessions, dropped and audited sessions, ICMP sessions, and half-open TCP sessions. (See Lewis et al. pages 6-7, Sections 0073-0082)

Referring to the rejection of claims 5 and 17, Jungck et al. as modified discloses wherein the predefined cache classes are assigned a priority for deletion (See Jungck et al. page 10, Section 0081)

Referring to the rejection of claim 6, Jungck et al. as modified discloses wherein the device is considered to be under network overload when the amount of memory used for session cache entries exceeds a configurable trigger threshold. (See Jungck et al. page 14, Section 0105)

Referring to the rejection of claim 7, Jungck et al. as modified discloses wherein a sufficient amount of memory has been freed when the amount of memory used for session cache entries falls below a configurable floor threshold. (See Jungck et al. page 25, Section 0177)

Referring to the rejection of claims 8 and 18, Jungck et al. as modified discloses wherein a memory usage threshold is configurable for each predefined cache class. (See Jungck et al. page 17, Section 0121)

Referring to the rejection of claims 9 and 19, Jungck et al. as modified discloses wherein said step of selecting and deleting includes the steps of:

retrieving from a database the amount of memory used to store session cache entries for each cache class (See Jungck et al. page

recognizing each cache class whose memory usage exceeds an associated memory usage threshold (See Jungck et al. page 25, Section 0177)

ordering each cache class according to its deletion priority (See Jungck et al. page 24, Section 0169)

selecting for deletion according to said ordering step some fraction of entries of a given cache class if said deletion brings said total cache memory usage below said floor, wherein, otherwise, all entries of said given class are selected for deletion (See Lewis et al. page 12, Section 0120, page 13, Sections 0130 and 0136)

continuing said step of selecting for deletion until it is determined that either deleting all the entries selected for deletion would bring the total cache memory usage below the floor threshold, or all entries in all defined cache classes have been selected for deletion (See Jungck et al. page 24, Section 0167)

Referring to the rejection of claims 10 and 20, Jungck et al. as modified discloses herein said step of ordering includes ordering cache classes whose memory usage does not exceed said associated memory usage threshold (See Jungck et al. page 21, Section 0152)

Referring to the rejection of claim 11, Jungck et al. as modified discloses herein configuration data for the thresholds may be supplied in a normalized fashion and be adaptively applied to the device, depending on the amount of memory on the device (See Jungck et al. page 15, Section 0115)

Referring to the rejection of claim 13, Jungck et al. as modified discloses wherein information kept in the memory management database is updated each time a new cache entry is created or deleted by the device (See Jungck et al. page 27, Section 0193)

Referring to the rejection of claim 21, Jungck et al. as modified discloses herein the pruning mechanism operates by making only one pass through a list of session cache entries in said device. (See Lewis et al. page 5, Sections 0063-0064)

Referring to the rejection of claim 22, Jungck et al. as modified discloses wherein a trigger threshold and floor threshold corresponding to said total memory usage are adjustably configurable (See Lewis et al. pages 8-9, Sections 0102-0104)

Referring to the rejection of claim 23, Jungck et al. as modified discloses wherein the memory usage statistics are collected using the Simple Network Management Protocol (SNMP). (See Lewis et al. page 4, Section 0047)

Referring to the rejection of claim 24, Jungck et al. as modified discloses wherein the pruning mechanism, when it has to delete some fraction of the entries in a given cache class, approximates the fraction b/t (where b is the total number of bytes of memory that must be freed and t is the total number of bytes of memory used to hold session cache entries for that cache class) with another fraction p/q, where p 7=1 and q is likely to be small relative to the total number of cache entries in that class; and then frees p entries out of every q entries in that cache class on the list of session cache entries (See Jungck et al. page 29, Sections 0200-0201 and page 30, Sections 0206-0216)

Referring to the rejection of claim 26, Jungck et al. as modified discloses wherein said prune selector is operable to selectively prune sessions of an ordered overlimit class if the memory used by said class is greater than the difference between a global

ceiling threshold and a global floor threshold. (See Lewis et al. page 12, Sections 0127-0130)

Referring to the rejection of claim 27, Jungck et al. as modified discloses wherein said prune selector is operable to prune all sessions of said overlimit class if the memory used by said class is less than the difference between said global ceiling threshold and said global floor threshold. (See Lewis et al. page 13, Sections 134, 136-137)

Referring to the rejection of claim 28, Jungck et al. as modified discloses wherein a next highest priority class is examined to determine if memory used by said class is greater than a remaining difference between said global ceiling threshold and said global floor threshold, said next highest priority class being selectively pruned if said difference is greater than said remaining difference. (See Lewis et al. page 13, Sections 0136-0137)

Referring to the rejection of claim 29, Jungck et al. as modified discloses wherein said prune selector is operable to prune all sessions of said next highest priority class if the memory used by said class is less than said remaining difference. (See Lewis et al. page 11, Sections 01118-0121)

Referring to the rejection of claim 30, Jungck et al. as modified discloses wherein said devices are selected form the group consisting of: network firewalls, routers, switches and hosts. (See Jungck et al. page 21, Sections 0148-0149)

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CDF
cdf
October 16, 2005

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137